BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	CG Docket No. 17-59
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	WC Docket No. 17-97
	)	
	)	

Comments of Noble Systems Corporation

Directed to the Commisions' Third Further Notice of Proposed Rulemaking (Call Blocking in a SHAKEN/STIR Framework)

Filed July 24, 2019

Karl Koster
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338

Chief Intellectual Property and Regulatory Counsel

I. Introduction

Noble Systems Corporation ("Noble Systems") [1] submits these comments in regard to the Commission's Third Further Notice of Proposed Rulemaking ("FNPRM").[2] Noble Systems supports the Commission's attempts to address the issue of eliminating illegal calls and recognizes that the Commission has identified many relevant issues in the FNPRM related to blocking calls in a SHAKEN/STIR ("S/S") framework. However, it is evident at this junction, there is a likelihood of confusion due to, in part, use of diverging terminology from that used in the S/S framework.

First, the Commission should align their descriptions of particular issues by using the terminology and concepts used by the ATIS/SIP Forum as found in the ATIS/SIP Joint Standard.[3] Second, the Commission should recognize the concepts for describing call blocking services in a S/S context are distinct from those describing call blocking in an analytics-based context. For example, the S/S framework does not inform which calls are "illegal" or "unwanted," but does use a precise set of terms that can be used to categorize certain types of calls. The S/S framework allows issues to be discussed with precision and clarity, and avoids countless hours of debating nebulous terms, such as the scope of "unwanted" calls or "reasonable algorithms."

The ATIS/SIP Joint Standard defines various aspects of processing a call, and recognizes that its processing may be one of many inputs to a carrier's optional call blocking service, but the ATIS/SIP Joint Standard does not specify any particular call blocking service. Similarly, the ATIS/SIP Joint Standard does not define the particulars of an analytics-based process (called "call validation treatment" or "CVT"), but recognizes it also may be a part of the S/S deployment. Finally, the ATIS/SIP Joint Standard does not define the means how an originating service carrier performs the determination of the legitimacy (authentication) of an indicated calling party number, which is used to determine the attestation level in the SIP INVITE Identify header.

---

[1] Noble Systems is an international manufacturer of contact center software and a hosted provider of contact center related services, with 30+ years' experience in the contact center industry. Noble Systems provides multi-channel processing, voice and data analytics, workforce management, robotics processing automation, and other related services.

[2] Public Notice: Consumer and Governmental Affairs Bureau and Wireline Competition Bureau Announce Comment Dates for Call Blocking and Caller ID Authentication Third Further Notice of Proposed Rulemaking No. 17-59, DA 19-597 (June 26, 2019).

[3] Joint ATIS/SIP Forum Standard, ATIS 1000074, Approved January 5, 2017 ("ATIS/SIP Joint Standard").

The Commission refers to call blocking as a monolithic service, but it should recognized that there are numerous variations. The Commission should clarify which aspects of a call blocking service in a S/S context are viewed as mandatory, recognizing this service may be distinct from call blocking services operating in other contexts. Once certain fundamental aspects of call blocking services are clarified, then the need for a "critical list" and the concept of a "safe harbor" can be better understood.

The Commission recognizes that carrier-based call blocking services are optional, whether the consumer opts-in to the service or has the option to opt-out from a default call blocking service. However, the Commission should mandate that carriers offering any type of call blocking service provide transparency to both the calling/called parties involved. Specifically, the concept of transparency includes providing a real-time per-call notification informing the calling party that their call has been blocked. While the Commission has allowed call blocking services in the past to be offered without this type of notification, this should be mandated for when call blocking services operate using S/S processing outputs. Many commentators have repeatedly informed the Commission of the importance of this aspect, and it is time for the Commission to signal to the industry that this will be a mandatory part of call blocking services in the future.

The following comments are divided into two parts. Part II is a high level discussion of various concepts and terms, and how they should be used to frame the issues. Part III addresses various particular paragraphs.

II. A Common Understanding of the Terminology and Concepts is Fundamental To Addressing the Issues

a. The Vocabulary Used for Analytics-Based Processing is Not Directly Applicable to S/S Processing

The Commission is well aware of numerous past comments addressing certain prior terms which are inherently ambiguous and the use of which has hampered discussions. For example, the term "robocall" may be appropriate for referencing the general problem of "unwanted" calls, but when it is necessary to evaluate a particular fact pattern, that term is ambiguous and not very useful.[4]

[4] The Commission, the FTC, and various state statutes all define the term "robocall" differently.

In the context of analytics-based call labeling and call blocking, an expanded vocabulary was adopted, comprising such as terms comprising "illegal/legal" calls and "wanted/unwanted" calls. While such terms may be useful at a high level, at their core they are inherently ambiguous and do not advance discussion. The S/S framework allows for greater precision and using its terminology is far more likely to result in a meaningful description of the context. Thus, the Commission is urged to be cognizant that various concepts used to describe analytics-based call blocking are not necessarily applicable to S/S call blocking. At a recent Commission hosted SHAKEN/STIR Summit, one speaker emphatically stated "SHAKEN/STIR **can not** help to determine the illegitimate vs. legitimate intent or content of the call."[5] Thus, framing questions as involving "legal" or "illegal" calls is not useful.

The S/S framework is a deterministic process for processing calls. A call blocking service based solely on processing S/S verification results is fundamentally distinct from a call blocking service operating on analytics, and the vocabulary is not interchangeable. The ATIS/SIP Joint Standard is largely devoid of characterizing whether a call is "wanted/unwanted", "legal/illegal", and avoids using other phrases that are associated with analytics-based blocking (such as referencing a "reasonable algorithm"). Keeping these concepts distinct and using a precise vocabulary facilitates understanding the particular issues being identified in the FNPRM.

b. "Authentication" in the S/S Framework

The ATIS/SIP Joint Standard describes itself as a document that "defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework."[6] Although sometimes colloquially referred to as the "SHAKEN/STIR Caller ID authentication framework"[7], this is imprecise, and is symptomatic of misunderstanding the concept of "authentication" as used in the ATIS/SIP Joint Standard.

The ATIS/SIP Joint Standard provides a diagram of the reference architecture shown below:

[5] FCC Hosted "SHAKEN/STIR Robocall Summit, July 11, 2019, comments by Chris Wendt, https://www.fcc.gov/SHAKENSTIRSummit at 7minutes 30 seconds, emphasis in original.
[6] ATIS/SIP Joint Standard, p. 1.
[7] See, e.g., par. 45 FNPRM.

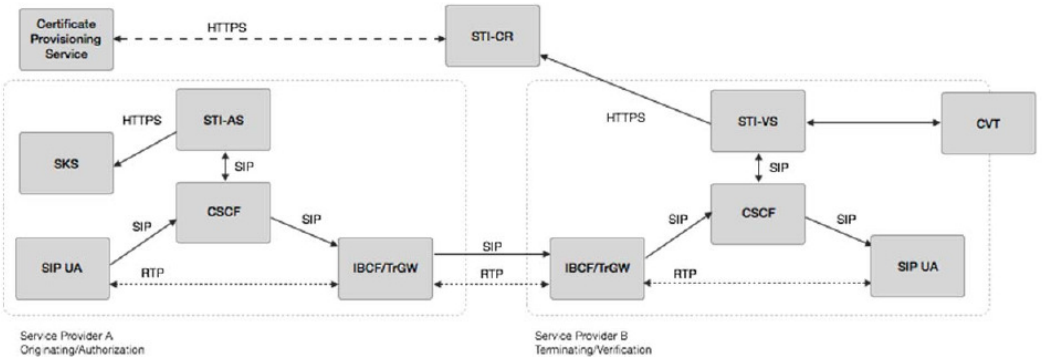


Figure 4.1 – SHAKEN Reference Architecture

The left side (denoted by the dotted line rectangle) represents processing by the originating service provider, referred to as Service Provider A. The SIP UA (SIP User Agent) can be embodied as end-user equipment (e.g., a PBX) and the other components in the rectangle can be embodied as various forms of carrier network equipment. Similarly, the rectangle on the right side is the terminating provider, referred to as Service Provider B.

The ATIS/SIP Joint Standard references the originating provider as performing "authentication" procedures.[8] The STI-AS function in Service Provider A is the "Secure Telephone Identify Authentication Service"[9] and is described as "[t]he SIP application server that performs the function of the authentication service defined in draft-ietf-stir-rfc447bis."[10]

A notable sentence in the ATIS/SIP Joint Standard states that "[t]he STI-AS in the originating SP (i.e., Service Provider A) first determines through **service provider-specific means** the legitimacy of the telephone number identity being used in the INVITE."[11] Thus, the originating service provider receives the call setup INVITE message that indicates the calling party telephone number and determines - according to its own defined procedures - whether the number is legitimate. This allows a service provider great flexibility determining how to determine the proper level of attestation (i.e. authenticate the number).

[8] Although FIG. 4.1 of the ATIS/SIP Joint Standard uses the word "authorization" in the diagram, the documents primarily uses the term "authentication." See e.g., Section 5.2, "4474 bis Authentication procedures."
[9] ATIS/SIP Joint Standard, page 3.
[10] ATIS/SIP Joint Standard , page 5.
[11] ATIS/SIP Joint Standard, page 6, Section 4.3, step 3, emphasis added.

The ATIS/SIP Joint Standard recognizes that flexibility is needed for how authentication occurs. An example can illustrate why this is needed. Consider a business (who is a customer to Service Provider A) that is originating appointment reminder calls to patients on behalf of medical providers in a service area. The business may "spoof" the corresponding telephone number of each medical provider as required. The business may contract and warrant to Service Provider A that each call it originates will convey a telephone number that the business has been authorized by the corresponding medical provider to use. In other words, the business is authorized to spoof numbers by its clients, and warrants to Service Provider A that it has the authority to do so. The procedures used by Service Provider A to vet the business are not defined in the ATIS/SIP Joint Standard. As long as Service Provider A is confident of the legitimacy of the number, it can assign a "full attestation" level to the number received. If Service Provider A is not confident of the legitimacy of the number, then it can assign a "partial attestation" level to the number. Service Provider A knows that because S/S calls can be readily traced, it will bear part of the risk if any "inappropriate" calls originate. Service Provider A may even require in its terms of service that no illegal calls will originate (however that may be defined), and the parties may contractually agree that Service Provider A may terminate service if that occurs. After the level of attestation is determined for a call, the Service Provider then uses its private key to sign the call, and adds the Identity header into the SIP INVITE message. Thus, the ATIS/SIP Joint Standard describes "authentication" as a process occurring only in the originating service provider.

Once the call reaches the terminating service provider (Service Provider B), the STI-VS or "Secure Telephone Identify Verification Service"[12] verifies the signature. This verification service is defined as "[t]he SIP application server that performs the function of the verification service defined in draft-ietf-stir-rfc4474bis."[13] Thus, verification occurs at the terminating carrier.

In regard to analytics-based processing, the SHAKEN Reference Architecture recognizes, but does not define, the specifics of the analytics-based processing. Namely, the "CVT" or "Call Validation Treatment" is defined as "a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that

[12] ATIS/SIP Joint Standard, page 3.
[13] ATIS/SIP Joint Standard, page 5.

indicates how the results of the verification should be displayed to the called user."[14] The ATIS/SIP Joint Standard otherwise does not mandate nor limit the CVT functions.

Similarly, the SHAKEN Reference Architecture does not mandate, nor define, a call blocking service based on any outcome of the terminating carrier's verification processing, but the ATIS/SIP Joint Standard does recognize that call blocking could occur.[15] However, as discussed below, there are many variations of call blocking services that a carrier could offer and it useful for the Commission to describe basic aspects of such a service when discussing issues related to call blocking in a S/S framework.

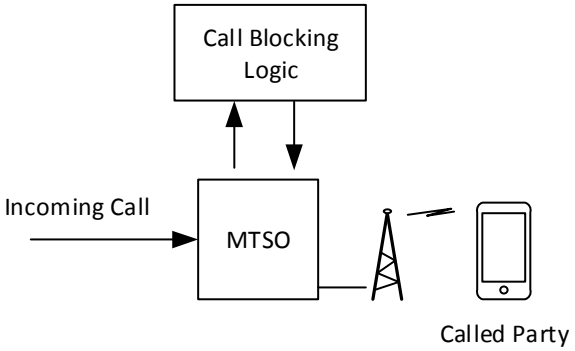
To summarize, the SHAKEN Reference Architecture refers to "authentication" processing as occurring only in the originating service provider, and "verification" processing as only occurring in the terminating service provider. The application of "analytics" and "call blocking" are optional and distinct services outside the scope of the SHAKEN call processing standards.

This understanding raises a fundamental question as to the Commission's definition and understanding of "authentication." The FNPRM states: "A call is then authenticated when the terminating provider checks the attestation information against the originating or gateway provider's certificate." [16] According to the ATIS/SIP Joint Standard, this is the process of verification, not authentication. The authentication process occurs in the originating service provider, not the terminating provider. Having a consistent understanding aids in avoiding confusion.

c. Call Blocking Services

Neither the ATIS/SIP Joint Standard, nor the FNPRM, define the scope of a call blocking service. There are numerous variations of call blocking services that can be defined. It is helpful to discuss three main types as a basis for comparison, illustrated using the exemplary figure below:

[14] Id.
[15] See, e.g., p. 4.
[16] Par. 47.



In one embodiment of an "analytics-only-based" call blocking service (referred to herein as "Type 1" call blocking), the incoming call is received at a mobile telephone switching office ("MTSO"), and the calling party number and the called party number are provided to the call blocking logic, which is executed by an analytics provider. Proprietary algorithms are used to determine the call disposition, and the MTSO is informed of the outcome. This reflects one embodiment of presently available call blocking services.

In an "S/S-based" call blocking service (referred to herein as "Type 2" call blocking), the incoming call is processed using the S/S procedures. Assuming the incoming call is signed, the MTSO performs the S/S processing and provides the verification outcome to the call blocking logic, which determines the outcome solely on the S/S event outcomes. This could implement a call blocking service where e.g., all gateway-attested calls are blocked, or only fully-attested calls are passed.

In a "hybrid-based" call blocking service ("Type 3" call blocking), the incoming call is received, and the MTSO performs the S/S processing, and the output of the S/S verification process, along with the calling/called party numbers, are used by the call blocking logic. In this case, the S/S outcome is merely another input to the algorithm, along with the calling/called numbers, and various other parameters. This version is similar to the analytics-only based processing (Type 1), in that a proprietary algorithm is used, the exact details of the processing are likely to be kept confidential, and the process will be difficult to precisely regulate.

It is possible to define a myriad of variations of each service. For example, in the "analytics-only-based" version (Type 1), a carrier could allow a called party to define a whitelist of numbers that should never be blocked, and/or a blacklist of numbers that should always be blocked. Or, a carrier could provide a very specific service of, e.g., blocking all telemarketing calls except those from e.g., automotive dealers. Likely, the carriers and analytics providers would

like the freedom to innovate as to how these services should operate to meet market needs. Based on experience and market experience, these services will likely evolve from their current form.

These variations could also be defined for the S/S-based and hybrid-based call blocking services. For example, a carrier could offer a call blocking service where all unsigned and gateway calls are blocked, except for calls purporting to be from a number on the called-party's whitelist, and only when offered prior to 10:00 p.m.

Although not formalized, it appears the only significant restrictions the Commission has placed on call blocking services to date are the following:

- if blocking is provided on an opt-in basis, the consumer must be fully informed of consequences, i.e., which types of calls will be blocked,
- if blocking is provide on an out-out basis, the consumer must be able to opt-out from receiving blocking,
- voice service providers should "avoid blocking calls from 'public safety entities, including PSAPs, emergency operations centers, or law enforcement agencies.'"[17]

At a high level, the only distinction between the current "analytics-only-based" form of call blocking and the "hybrid-based" call blocking service is that the latter uses an additional input –the output of the S/S verification process. It would not make sense for the Commission to impose different restrictions on these two carrier services. Thus, if the Commission intends to impose a requirement on defining a 'critical call list' for the hybrid-based call blocking service, it should also be mandated for other call blocking services. Otherwise, this would result in difficulties in enforcement and confusion to consumers. There is little distinction between an analytics-based algorithm which does not receive the results of a S/S verification process (Type 1) and analytics-based algorithm (Type 3) which does receives the results, but which may ignore the input.

One call blocking service characteristic that the Commission should mandate carriers to provide involves providing transparency to the calling/called parties of which calls are blocked. The caller should be informed the call was blocked via an audio intercept to the caller and returning a suitable error/cause code in the signaling. The audio intercept should convey a telephone number and/or a website address where the caller can challenge the blocking of the call. The carrier must

[17] Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Federal Register, vol. 84, No. 121, Monday June 24, 2019, page 29388.

provide a suitable contact channel for receiving and addressing these requests in a timely manner, both from the consumer (the called party) and the calling party. Segments of the industry have repeatedly requested this capability, and it is appropriate for the Commission to mandate this functionality, including retroactively requiring it for analytics-only based call blocking services (Type 1).

d. S/S-Based (Type 2) Call Blocking May be Overbroad

Blocking calls using only the results of S/S verification results may result in over-blocking, particularly in the early stages of S/S deployment. Thus, this service should be used with caution, as consumers may find it undesirable. In these use cases, it is not possible to know whether the call is "wanted" or "legal" and such descriptions are not very useful in this context. Further, the relative number of calls covered by a particular S/S blocking service will change over time as deployment progresses.

For discussion purposes, several potential use cases are describe below. In the following nomenclature, "A" refers to the calling/originating side, and "B" refers to the called/terminating side of the call.

1. **End-to-End VoIP call**. Caller A's number is fully attested and signed by Service Provider A, and the call is routed to Service Provider B, where it is verified before being offered to Called Party B. It is unclear whether such a call is necessarily "wanted" or "legal," but it can be ascertained with precision that the number is not an unauthorized spoofed number.
2. **SS7 Call to VoIP Called Party**. Caller A is a rural telephone subscriber originating a conventional telephony call (i.e., "SS7 Call") to a VoIP-based Called Party B. The call will be interworked at some point at a gateway and converted to VoIP (e.g., SIP). If the gateway is upgraded to perform S/S processing, then the SIP INVITE message will include an Identity header with gateway attestation. If the gateway is not upgraded to insert an Identify header, then the SIP INVITE will be generated without the Identify header and the call will be an "unsigned" call. If Called Party B elects to block all unsigned or gateway attested calls, then such calls will be blocked.
3. **Overseas Scam Call to VoIP Called Party**. An overseas scammer originates a call and spoofs a domestic telephone number. At some point the call will reach a gateway

and the call will be processed similar as described in the above use case. The call will either be unsigned or it will have an Identity header reflecting gateway attestation. If Called Party B elects to block all gateway attested calls, then such calls will be blocked.

It should become apparent that in the context of S/S only, certain calls, such as gateway attested calls cannot be clearly ascertained as "wanted" or "legal" calls. The mere fact that the call is unsigned does not mean it is unwanted/illegal. It may be that the gateway was not upgraded to sign the call. In addition, signed calls could have their Identify header 'stripped off' by transit carriers, where equipment is not upgraded to properly handle SIP INVITE messages which exceed a certain size.

It is recognized that analytics (i.e., Call Blocking Type 3 services) may be able to better distinguish between use case #2 and use case #3. It should be further recognized that as S/S is deployed more widely (i.e., more SS7 networks are converted to VoIP or otherwise S/S enabled), then there will be fewer domestic originated unsigned calls and domestic "gateway attested" calls. Thus, the need for analytics to distinguish between these two use cases may diminish in future.

The industry does not have any collective experience as to how quickly deployment of S/S will occur and what type of issues will arise. Thus, while domestic unsigned calls should diminish over time, it is unclear when this will reach a de-minimus volume. The only aspect that is known for certain is that the volume of such calls will change over time. Thus, the Commission should recognize the need for flexible regulations to accommodate evolution in network deployment.

There is one possible use case of blocking calls solely based on a S/S verification outcome that does not make sense. Specifically, it is not anticipated there would be a need for consumers to block fully attested calls (solely based on that criteria). If this conclusion is accepted, then it is germane to the analysis of whether a critical calls lists should be defined in a S/S call blocking service. (See infra.)

e. Safe Harbor

The concept of a safe harbor is basically that an entity can avoid liability provided if it performs certain actions. Creating a safe harbor in the context of a call blocking service offered by a terminating carrier requires clarification by the Commission. The Commission has recently

clearly indicated that blocking calls, by itself, is not a violation of a carrier's obligation to complete calls under section 201(b) of the Communications Act. Specifically:

> 2. The Commission has repeatedly stated that offering call-blocking services does not violate voice service providers' call completion obligations under section 201(b) of the Communications Act of 1934, as amended (the Act), and that consumers have a right to block calls. Nonetheless, uncertainty regarding when voice service providers may implement call-blocking programs remains. The Commission issues the *Declaratory Ruling* to resolve uncertainty and make clear the call-blocking tools that voice service providers can offer.

In the Commission's 2015 Order addressing call blocking, the Commission has imposed very limited obligations on a carrier to avoid liability.[18] The Commission stated:

> 157. We clarify that services that allow consumers to designate categories of incoming calls (not just individual telephone numbers) to be blocked, such as a "telemarketer" category, also constitute consumer choice within their right to block calls.… Regardless of how a blocking technology obtains the individual phone numbers within these categories, a consumer may choose to subscribe to a blocking service **as long as** the carrier offering the service or coordinating with the technology provider adequately discloses to the consumer the risks of inadvertent blocking. (Emphasis added.)

Thus, it appears a primary obligation of the carrier is that it must adequately disclose the risks of "inadvertent blocking" to the consumer. In an analytics-based environment (for which the 2015 Order pertains), the algorithms were recognized to be imperfect, and that occasionally wanted calls would be blocked. Thus, the concept of "inadvertent blocking" is applicable. Provided the carrier meets the disclosure obligation, the carrier avoids liability for over-blocking calls. This disclosure requirement appears to be an existing safe harbor requirement for carriers blocking calls. *Fundamentally, the Commission cannot broadly state "consumers have a right to block calls" and then attach liability to the carrier for blocking calls as requested by the consumer.*

The Commission should clarify that this safe harbor disclosure obligation is required for opt-out and in all other forms of call blocking services. The consumer should be provided suitable information to know exactly what types of calls will be blocked. Assuming the Commission

[18] Declaratory Ruling and Order, FCC-15-72A, Released July 10, 2015.

intends this disclosure obligation to be a safe harbor to avoid liability, then it would bolster the argument that this obligation is applicable to any form of call blocking service. Failure to do so would highlight the arbitrariness and consumer confusion that can arise if the Commission were to impose different disclosure obligations on different types of call blocking services.

There are other aspects of a call blocking service that the Commission has not addressed (which may warrant another rulemaking proceeding). For example, in addition to addressing requirements of disclosure and transparency, there are aspects of mitigation that the Commission has not addressed. If consumers are to be given the ability to review calls that have been blocked, and inform the carrier of a potential mistake (i.e., that a particular call was incorrectly blocked and should be offered in the future), then that implies the carrier is required to maintain a specific exception list for that called party. To illustrate, a consumer may receive calls from a relative ("Aunt Bee") in a rural area ("Mayberry") that are blocked because the calls are not signed, or if signed, they are received with a gateway attestation indication. The consumer may have elected to have all unsigned calls and/or gateway attested calls blocked (which results in blocking calls from Aunt Bee). The consumer may report this blocked call as a wanted call to their carrier. If the consumer is to be accommodated, then, for that particular calling party number, the carrier should not block calls from Aunt Bee. Thus, an exception is created for that consumer. Obviously, other consumers (not related to Aunt Bee) would probably not desire to have Aunt Bee's number on their exception list, but create their own personalized list. In this hypothetical, carriers providing a call blocking service now require to maintain an exception list for each consumer.

Whether a consumer exception list is to be mandated for each type of blocking service for each called party has not been squarely addressed by the Commission. The Commission has alluded to defining a "Critical Calls List" and a "whitelist", which are examples of exception lists, but which appear to be defined at a federal, state, and/or local level. It would be beneficial to first have an understanding of what are the overall requirements for a call blocking service before addressing a particular instance. Presumably, these would be defined as safe harbor requirements to avoid liability under section 201(b).

The Commission appears to be intimating that other actions may be required by the carrier to obtain a safe harbor. These actions appear to now essentially dictate the criteria on which calls will be blocked, i.e., the fundamental call blocking logic or algorithms. For example, the Commission "propose[s] a safe harbor for voice service providers that offer call-blocking

programs that take into account whether a call has been properly authenticated under the SHAKEN/STIR framework and may potentially spoofed….Many have asked us to provide a safe harbor for the blocking of calls that are likely to be illegal."[19]

First of all, to precise, it appears that the intent of the proposal is based on whether the call was properly *verified* by the terminating service provider (not authenticated by the originating service provider). The scope of this requirement raises various questions. What is the distinction between a "verified" call versus an "improperly verified" and a "properly verified" call? An unsigned call cannot be verified one way or the other. When a signed call is received, it is presumed that (in most cases) the public key can be used to verify the call (i.e., it is not corrupted or expired). Once the signed call is verified, the information in the attestation indicator can be relied upon, and will indicate one of: gateway, partial or full attestation. A verified call that indicates gateway attestation (or any other level) should not be considered as "improperly" verified. Categorizing such a call as illegal or likely illegal should be avoided. On the other hand, if the contents of the Identify header were tampered with or the certificate has expired, then the call cannot be verified (and should not be described as an "improperly verified" call, but as an unverifiable call). Thus, the terminating service provider may output the result of: a) unsigned or unverified calls, b) signed and verified calls, and c) signed and unverified calls.

Assuming the Commission is referring to the last case as a call that is not "properly verified", the carrier may offer a blocking service to the consumer to block calls that are signed and cannot be verified. Such calls may not be verified because of a e.g., a transmission error corrupting the Identify header, use of an expired certificate, a communications failure in the verification service in retrieving the public key, etc. The Commission has clearly stated that there is no violation of the carrier's call completion obligation in blocking such calls (provided there are adequate disclosures to the consumer of which calls will be blocked). Thus, if the consumer stipulates blocking all unverifiable calls, there is no liability for the carrier doing so. Consequently, it is unclear in this instance what exact form of safe harbor the Commission is proposing. Is the Commission considering withdrawing its statement that blocking of calls is not a *per se* violation of the carrier's call completion obligation?

Imposing additional requirements on the call blocking service can quickly lead to a quagmire of needless complexity. Consider a carrier that offers a Type 1 (analytics-based) call

[19] Par. 46.

blocking service, where the consumer requests certain types of calls to be blocked (i.e., scam calls). This analysis is based solely on the calling/called party numbers. In this case, a particular call meeting certain proprietary determined criteria will be blocked, and the carrier can do so without violating their call completing obligations. Now consider a carrier offering a Type 3 (hybrid-based call blocking) service. The call blocking logic receives both the calling/called party numbers, and an indication of the S/S verification outcome. The algorithm may determine based solely on the calling/called party numbers that the call meets the scam call type. In this case, the algorithm may block the call, effectively disregarding the verification results. Does the carrier lose the benefit of a safe harbor in blocking the call because it did not "properly consider" the verification results? Should liability depend on whether the algorithm "properly" considers the verification output? The difference in the call blocking logic in this example compared to that occurring in Type 1 example may be de-minimus.

f. A New Safe Harbor Provision Should be Defined

There is one important instance of a safe harbor that the Commission does not address. The principle of equity requires that a terminating carrier blocking a call should not be liable for blocking calls based on mistakes made by an originating carrier. A terminating carrier may be asked by a consumer to block a particular form of S/S call, e.g. a gateway attested call or an unverifiable call. An originating carrier may mistakenly authenticate the call as a gateway attested call, or, the originating carrier may use an obsolete certificate. If the called party has requested blocking of gateway attested calls or unverifiable calls, then call is expected to be blocked.

The terminating provider is doing exactly what was requested by/promised to the called party, and the terminating provider should not be liable for blocking the call. The safe harbor is predicated on performing the call blocking as requested. If, however, the terminating provider does not perform as promised, (e.g., it blocks a fully attested call which the consumer did not request), then the terminating provider should be liable. That is, there is no safe harbor to carriers failing to do what was promised. On the other hand, if the originating service provider improperly authenticates the call, the originating service provider should not receive a safe harbor for making such a mistake. No carrier would agree to accept liability for mistakes made by another carrier,

nor would principles of equity allow this.[20] The Commission should use these basic concepts in redefining a simple framework of what activities are required by a carrier to avoid liability.

III. Comments On Specific Paragraphs

In general, the Commission should review usage of the term "authentication" in the FNPRM and align its use with the ATIS/SIP Joint Standard.

a. Par. 46

The S/S framework allows ready identification of *unauthorized* spoofed numbers (i.e., partially attested). It is possible, and expected, that callers who are authorized to use another entity's number (such as entities that originate calls on behalf of others), may have their calls indicated as "fully attested." Callers that spoof numbers on an *unauthorized* basis should have their calls authenticated as "gateway attestation" or "partial attestation." Terminating carriers that agree to block these specific types of signed calls, and do so as promised, are not liable according to the Commission's most recent order. Carriers should receive a safe harbor for processing the call as promised and providing associated call transparency functions when blocking calls.

b. Par. 47

This paragraph states "A call is then authenticated when the terminating provider checks the attestation information against the originating or gateway provider's certificate." The definition of "authentication" is at odds with the concept as defined in the ATIS/SIP Joint Standard. The terminating service provider performs a verification service.

c. Par. 48

Reference to calls that "fail Caller ID authentication" appears to have intended to refer to calls that fail verification at the terminating service provider. Verification can "fail" or be unsuccessful due to e.g., transmission errors in the Identify header, maliciously altered information in the Identify header, equipment stripping off the Identify header, use of expired certificates, a failure to obtain the STI-CR URI, etc. It is inaccurate to categorize such calls are "illegitimate"

[20] Indeed, the terminating carrier cannot identify whether the originating carrier assigned an incorrect attestation level.

and presume that they should be blocked on that basis. It is recommended that only after experience is obtained with deployment and understanding the relative frequency of such events that the need for blocking such calls should be reviewed.

d. Par. 49

A terminating carrier promising a called party to block all calls that fail S/S verification should not be liable for providing such a service and blocking such calls in light of prior Commission Orders. In the specific instance where blocking is due to the originating carrier failing to ensure their public key infrastructure is current, the terminating carrier should not be liable since it acted as it promised and performed the procedures according the S/S framework. The fault lies with the originating service provider and there is no reason why the originating carrier should receive a safe harbor for being negligent by failing to update its public key infrastructure.

The Commission should also at this time avoid attempting to categorize certain calls in S/S framework as being illegal. A call that "fails authentication" (i.e., fails verification) may be due to a technical issue as opposed to actions of a malicious actor. Until experience is gained with deployment and carriers have a better understanding of potential problems and their frequency, it is not useful to presume any type of failure in verification is due to malicious actors or that such calls are illegal. Likely, the nature of these verification failures will drastically change as S/S deployment progresses and experience is gained.

e. Par. 50-51

The Commission implies that only calls for which attestation is available (i.e., signed) "and that fail authentication would be blocked." Presumably the Commission means that only signed calls that fail *verification* would be blocked. Terminating service providers would likely expect the flexibility to offer blocking services as consumers demand. Thus, a carrier may offer a service elected by a consumer, for example, that redirects all gateway attested calls (which are not considered as failing verification) to a voicemail system, but allows all other calls to be offered. In this case, certain calls which passed verification could be viewed as blocked while certain other calls which passed are allowed.[21]

[21] This raises a separate issue of whether diverting a call should be considered the same as blocking a call.

It should be noted that many consumers may be unpleasantly surprised if they elect a call blocking service that only blocks calls based on the S/S verification outcome (i.e., a Type 2 call blocking service). Likely, under this call blocking service definition, many important (i.e., "wanted" and "legal") calls will be blocked. Carriers cannot discriminate which calls are "wanted" and "legal" solely based on S/S processing outputs. In contrast, carriers can discriminate all "gateway attested" calls from "fully attested" calls and do so with 100% certainty.

The Commission has previously stated that carriers can block calls for their subscribers without violating the call completion obligations. If the service provider is blocking calls in the manner as they informed the consumer, then according to the Commission, they would not be liable.

f. Par. 52

Carriers that do not sign calls will be very quickly placed at a significant competitive disadvantage. Their customer's calls will be unsigned and their calls will have decreased answer rates relative to signed calls when terminating on a S/S enabled carrier. Customers will demand carriers to sign their calls or they will elect to use another available carrier. Noble Systems has already observed concern from contact center operators on this point. Thus, market competition will incentivize carriers to sign their calls.

Thus, access to S/S certificates will be critical to the operation of the carrier, and it can be expected that carriers will police their customers in order to avoid having their certificates revoked or not renewed. Abusive callers will be readily identified, as will their carriers who knowingly tolerate such abuses. Carriers will be forced to exercise judgement as to their customers' call offering practices and carriers will use other means to encourage their customers to comply with legal calling practices. For example, a carrier may vet their customer before providing service for high volume, short duration call origination rates and require a contractual obligation that only numbers allocated by the carrier to the customer will be used. Or, the carrier may require a certification or warranty that any telephone numbers used by the customer are authorized by the end user of the number. The carrier may require a bond or deposit from a customer if the risk level warrants. Authentication is fundamentally an issue of trust, and businesses have ways for accommodating different levels of trust.

Because of the trace back feature, callers that abuse the use of numbers can be quickly identified, as will the carriers that willfully ignore such practices. Carriers that fail to properly police their customers may find that they are unable to obtain a renewal certificate, which would be economic disaster for that carrier. In the recent past, it was impractical to trace a few calls or even a few hundred abusive calls. As S/S is deployed, even a single abusive call may prompt the called party to report the caller, causing a trace back to occur that would identify the originating carrier. The motivation to be compliant will increase, and carriers will become another entity motivating callers to be compliant as well.

g. Par. 54

The Commission recognizes some of the various technical issues that can adversely impact the integrity of the Identify header in the SIP INVITE message. It should be recognized that the industry is not fully aware of all the potential problems can arise with S/S deployment, and that further experience will be gained as implementation progresses. Thus, blocking unsigned calls could (initially) result in many desirable calls being blocked. Likely, at some point in the future, sufficient information will be known to quantify the risks of blocking such calls. Carriers will likely be circumspect in offering call blocking services that will adversely impact their consumers.

The Commission's statement asking for setting a date certain for "when this type of blocking is permissible" implies that offering this type of call blocking service prior to this date would be impermissible. Specifically, since the Commission has indicated that a carrier can now block calls for a customer, why would it be presently impermissible for a carrier to block e.g., unsigned calls? It should be noted that while unsigned calls can be identified with 100% in a S/S framework, it is incorrect to presume the S/S can identify these as "illegal" calls. Again, as stated by one expert, "SHAKEN/STIR **can not** help to determine the illegitimate vs. legitimate intent or content of the call."[22]

h. Par. 55

Describing "wanted calls" has no precise meaning in the context of S/S. S/S allows identification of signed and unsigned calls, as well as identifying a level of attestation for signed

[22] FCC Hosted "SHAKEN/STIR Robocall Summit, July 11, 2019, comments by Chris Wendt, https://www.fcc.gov/SHAKENSTIRSummit at 7minutes 30 seconds, emphasis in original.

calls that can be verified. Blocking a call based on whether it is signed or its level of attestation can be done with certainty, but it is fruitless to attempt to categorize these are "wanted" or "legal" calls in the S/S framework. Thus, as S/S is deployed, the number of VoIP calls that are unsigned will decrease as domestic VoIP providers deploy S/S technology.

The Commission should mandate that any carrier offering a call blocking service must provide transparency to both the called party and the calling party. That is, real-time information must be available to the calling party that their call was blocked. This should be provided both as an audio intercept and an appropriate error/cause code returned to the caller. The calling party (and called party) should be able to access information in real-time as to what calls were blocked. In both cases, information should be provided to allow the parties to request mitigation of allegedly erroneous blocking. For the caller, information in the intercept can indicate a web site or telephone number to submit a mitigation request. For the called party, a portal can be accessed providing information about blocked calls and how to submit mitigation requests.

The Commission should recognize that the deployment of S/S by itself, without any form of call blocking, provides some mitigation with respect to the overall "robocall" problem. That is, as S/S deployment becomes more widespread, it facilitates trace back, which makes it harder for scammers to hide. Once scammers are identified, pressure can be made to bear on them and their carriers, and we can expect that will adversely reduce the call volumes. Further, as more and more S/S is deployed, blocking certain type of S/S calls will become more targeted and the level of attestation indicated on a call will become more useful. Thus, the Commission should realize that blocking solely based on S/S events is not necessarily required, nor useful, in the early stages of S/S deployment.

It is appropriate to mandate that carriers offering network-based call blocking services must offer caller notification and mitigation as a safe harbor. The experience of carriers offering analytics-based call blocking without such notification has created considerable disruption in certain industries. This was done, presumably, by the Commission to 'fast-track' deployment of analytics-based blocking of robocalls. Such fast-tracking of call blocking in a S/S framework is not needed, as deployment of S/S itself will address the problem in part. It is now appropriate for the Commission to put carriers on notice that call blocking services will require transparency of which calls are blocked and means to mitigate.

i. Par. 59-66

The Commission is implicitly defining aspects of a network-based call blocking service. First, during the early phase of S/S implementation, defining a call blocking service based solely on S/S verification outcomes (Type 2 call blocking service) has the potential of overblocking more calls than desired. It is not clear whether carriers would even want to initially offer such call blocking services using only S/S events as the basis for blocking. For example, blocking all unsigned calls in the early stages of S/S deployment will impact a larger proportion of calls initially than after several years, when presumably there will be fewer unsigned calls. As time progresses, fewer domestic calls will be unsigned or will be categorized as "gateway attested." It would appear prudent to discourage short-term wide scale call blocking until further experience is gained. Further, the Commission has stated that carriers can block calls at the consumer's request without violating their call completion obligations.

Second, the Commission appears to take a different approach to call blocking in these paragraphs that is difficult to reconcile with prior statements regarding call blocking. In the 2015 Order, the Commission stated:

> 154. We grant the Attorney Generals' request for clarification and clarify that there is no legal barrier to stop carriers and providers of interconnected and one-way VoIP services from implementing call-blocking technology and offering consumers the choice, through an informed opt-in process, to use such technology to block individual calls or categories of incoming calls that may be part of a mass unsolicited calling event. As such, we find that telephone carriers[23] may legally block calls or categories of calls at a consumer's request if available technology identifies incoming calls as originating from a source that the technology, which the consumer has selected to provide this service, has identified.[24]
>
> 157. We clarify that services that allow consumers to designate categories of incoming calls (not just individual telephone numbers) to be blocked, such as a "telemarketer" category, also constitute consumer choice within their right to block calls.… Regardless of how a blocking technology obtains the individual phone numbers within these categories, a consumer may choose to subscribe to a blocking service as long as the carrier offering the service or coordinating with the technology provider adequately discloses to the consumer the risks of inadvertent blocking.

[23] References in this section to "carriers" include VoIP providers, unless otherwise indicated.
[24] We do not distinguish between technology that blocks individual numbers or categories of numbers, or that relies on carrier-provided lists of numbers versus crowd-sourced black lists of numbers. For purposes of this statement of clarification, if the consumer is informed of the risk that the technology may inadvertently block desired calls (including both the existence of the risk and the approximate magnitude of the risk, where ascertainable), then nothing in our rules prohibits a carrier from offering a consumer the choice to use the technology.

Further, the Commission most recently affirmed that:

> 2. The Commission has repeatedly stated that offering call-blocking services does not violate voice service providers' call completion obligations under section 201(b) of the Communications Act of 1934, as amended (the Act), and that consumers have a right to block calls. Nonetheless, uncertainty regarding when voice service providers may implement call-blocking programs remains. The Commission issues the *Declaratory Ruling* to resolve uncertainty and make clear the call-blocking tools that voice service providers can offer.

Heretofore, it appears that as long as the consumer has been suitably informed, the carrier can block any call type the consumer desires. Now the Commission implies that certain emergency calls must never be blocked. To this end, the Commission discusses the creation of a "critical call list" or "whitelist."

If the Commission now intends to restrict call blocking services, the Commission should also apply any such restrictions apply to analytics-based network call blocking services (Type 1 call blocking services). The Commission cannot define one set of restrictions for network-based analytics-based call blocking and another set of restrictions for S/S triggered call blocking. It should be recognized that the S/S framework allows a CVT or analytics based function to be layered on top of S/S, so that the processing output of S/S can be another input to analytics-based blocking (Type 3 call blocking service). Thus, the distinction will be blurred creating further confusion about the requirements. Consequently, a restriction defined for a Type 3 service should also be applicable for a Type 1 service.

The Commission seeks to avoid blocking of emergency numbers by defining a "critical calls list" or "whitelist." First, it is certain that the scope of such a list will be difficult to define and maintain in secret. The key to stopping scammers spoofing emergency numbers is to deploy S/S technology ubiquitously and not rely on keeping the list secret. Creating such a list further needs an administrative body to process/update such lists. This critical call list represents another exception list of calls which should not be blocked (see earlier discussion). This list would appear to include nationally defined critical numbers, state defined critical numbers, and locally defined critical numbers. Further, if consumers have different views as to what is a "critical call" and should not be blocked, then this also suggests a consumer defined exception list. For example, if a parent views calls from a particular school as potentially critical, then they might want that number on their list, but another individual who does not have children in school would not. The scope of

call blocking can quickly grow to be complex and the management of a federal, state, local, and individual exception lists seems analogous to the infrastructure required to administrator the DNC list. The Commission should confirm if this is the direction intended to be pursued.

In paragraph 63, the Commission seeks comment on "limiting Critical Calls List protection to only those calls for which the Caller ID is authenticated. Does this provide protection against illegal callers spoofing crucial numbers?" Recall that authentication occurs by service-provider specific means in the originating network, and that verification occurs in the terminating network. Once a calling number is authenticated, then that means the call is signed with the corresponding attestation indication. Presumably, schools, government entities, and other critical callers will have a "full attestation" level when their calls are signed.[25] Consequently, these calls would be received as signed and fully attested, and such calls would be presumably verifiable (i.e., no obsolete or corrupted certificates are used). When such calls are validated as fully attested, there is no reason why they should be blocked by the terminating carrier on that basis. Recall that it does not make sense in a S/S framework to offer a call blocking service where fully attested calls are blocked on that basis. If the terminating carrier has not yet upgraded to S/S, then the carrier will not be blocking calls using the S/S processing as an input. Of course, the terminating carrier may be offering a Type 1 or Type 3 analytics-based call blocking service, and the Commission has stated that terminating carriers should avoid blocking emergency calls. In short, in the context of S/S call blocking, emergency calls should be fully attested and carriers would likely not block on this level of attestation. Thus, it is unclear why such a critical call list needs to be created in a S/S framework.

A more likely scenario is when the caller has their calls signed (fully attested) and an intervening network e.g., strips off the Identity header (as it is not yet capable of transmitting a lengthy SIP INVITE message), and the terminating network then processes that incoming call as an unsigned call. The terminating carrier may offer their subscriber a service that blocks all unsigned calls. This highlights the risk of encouraging carriers to block all types of calls, such as all unsigned calls. No doubt many other calls will also be blocked, and the network cannot readily tell which are wanted/unwanted/legal/illegal.

Another possibility involves a Type 3 blocking service. In this case, the fact that the call is fully attested would likely not be a factor in blocking the call, as the analytics algorithm may,

[25] These entities would not appear to have a need to spoof calls.

for whatever reason, determine that this call should be blocked regardless. Again, the Commission has stated that terminating carriers should avoid blocking emergency calls in an analytics-based call blocking context, and that admonition should still apply.

The Commission appears to be defining another nebulous category similar to "wanted" and "legal", namely that of "critical/non-critical." According to the Commission's statement that consumers have a right to block calls, provided that the consumer is fully informed of the risks of blocking such calls, then such practices are acceptable. As noted above, this may be a temporary situation, as once the S/S infrastructure is deployed, critical calls (i.e., police, emergency responders, etc.) should be signed and fully attested, and they should not be blocked because of their full attestation.

Noble Systems believes that call blocking solely based on S/S verification outcomes may overblock calls, and be harmful to consumers, more so in the short term. In the longer term, as S/S is more prevalent, blocking calls is more likely to be more accurately tailored to certain calls, less likely to overblock. Irrespective of call blocking deployment, as S/S becomes more prevalent, domestic bad actors can be more easily tracked and shut down. Restoring trust in voice calls is obtained by quickly identifying the bad actors and terminating their service, as opposed to merely blocking their calls and letting them continue with impunity.

IV. Conclusion

Identification of the issues and their resolution thereof would be facilitated by the Commission framing the issues with greater precision and explanation, along with aligning terminology used in the ATIS/SIP Joint Standard. The Commission should reconcile its recent statement that 1) voice service providers can offer call-blocking services without violating their obligations under Section 201(b) with 2) proposals in the FNPRM suggesting that such services are, in fact limited, and that blocking certain types of calls would be prohibited.

The Commission should clarify and distinguish limitations applicable to analytics-based algorithms only (Type 1), triggered on S/S events only (Type 2), or a hybrid combination thereof (Type 3); or whether the Commission intends to even distinguish between the technology and algorithms used by a carrier to trigger blocking when defining any limitations. It would be preferable that the Commission require any safe harbor requirement for one form of call blocking service to be applicable to all forms of call blocking services. The only additional mandate

applicable to all forms of call blocking service that the Commission should define at this time is that a carrier blocking calls must also provide corresponding notifications to calling and called parties, and provide a mechanism to mitigate blocked calls.

The Commission should recognize that triggering blocking of calls based solely on S/S verification outcomes will likely result in over blocking of calls in the early deployment of S/S, and should caution carriers from offering such services. Many non-S/S equipped carriers (i.e., conventional telephony carriers) will have their calls conveyed into VoIP service providers as either as unsigned calls or signed with a gateway attestation level. Blocking these calls may result in consumer missing more calls than anticipated.

Respectfully submitted on July 24, 2019,

/Karl Koster/

Karl Koster
Chief Intellectual Property and Regulatory Counsel,
Noble Systems Corporation
1200 Ashwood Parkway
Suite 300
Atlanta, GA 30338
(404) 851-1331
kkoster@noblesystems.com